

THE HONORABLE JAMES L. ROBART

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

STEVEN VANCE, *et al.*,

Plaintiffs,

v.

MICROSOFT CORPORATION,

Defendant.

No. 2:20-cv-01082-JLR

**DEFENDANT MICROSOFT
CORPORATION'S RENEWED
MOTION FOR SUMMARY
JUDGMENT**

NOTE ON MOTION CALENDAR:
June 10, 2022

ORAL ARGUMENT REQUESTED

TABLE OF CONTENTS

1		
2		
3	INTRODUCTION	1
4	UNDISPUTED MATERIAL FACTS	3
5	A. Flickr and the Yahoo-Created YFCC100M Dataset	3
6	B. The IBM-Created DiF Dataset.....	3
7	C. Plaintiffs’ Flickr Photos	4
8	D. Microsoft Contractor Benjamin Skrainka’s Download of the DiF Dataset	5
9	E. Microsoft Student Intern Samira Samadi’s Download of the DiF Dataset.....	8
10	ARGUMENT	10
11	I. BIPA Does Not and Cannot Constitutionally Apply to Microsoft’s Activities in	
12	Washington and New York.....	10
13	A. BIPA Does Not Apply Extraterritorially to Microsoft.	10
14	1. The Undisputed Facts Confirm Microsoft’s Relevant Conduct	
15	Occurred Entirely Outside Illinois.....	11
16	2. Microsoft’s Alleged BIPA Violation Had No Connection to	
17	Illinois.	13
18	3. Plaintiffs’ Illinois Residency Alone Cannot Satisfy Illinois’	
19	Extraterritoriality Doctrine.....	15
20	B. Applying BIPA to Microsoft’s Out-of-State Conduct Would Violate the	
21	Dormant Commerce Clause.....	17
22	1. Plaintiffs May Not Use BIPA to Regulate Conduct Occurring	
23	Outside Illinois’ Borders.....	18
24	2. BIPA’s Application Here Would Conflict with Washington and	
25	New York Biometric Privacy Law.	19
26	II. BIPA Section 15(b) Does Not Apply Because Microsoft Had No Way To Give	
27	Notice and Obtain Consent Before Downloading The DiF Dataset.	21
	III. The Court Should Grant Summary Judgment on the Unjust Enrichment Claim.....	23
	CONCLUSION.....	24

TABLE OF AUTHORITIES

Page(s)

Cases

<i>Chinatown Neighborhood Ass’n v. Harris</i> , 794 F.3d 1136 (9th Cir. 2015)	18
<i>Cleary v. Philip Morris Inc.</i> , 656 F.3d 511 (7th Cir. 2011)	24
<i>Corsello v. Verizon New York, Inc.</i> , 967 N.E.2d 1177 (N.Y. 2012).....	24
<i>Cousineau v. Microsoft Corp.</i> , 992 F. Supp. 2d 1116 (W.D. Wash. 2012).....	24
<i>Daniels Sharpsmart, Inc. v. Smith</i> , 889 F.3d 608 (9th Cir. 2018)	17, 18
<i>David K. Lindemuth Co. v. Shannon Fin. Corp.</i> , 637 F. Supp. 991 (N.D. Cal. 1986)	15
<i>Healy v. Beer Institute, Inc.</i> , 491 U.S. 324 (1989).....	18
<i>Hernandez v. Spacelabs Med. Inc.</i> , 343 F.3d 1107 (9th Cir. 2003)	13
<i>Hesketh v. Total Renal Care, Inc.</i> , 2021 WL 5761610 (W.D. Wash. 2021)	10
<i>Iancu v. Brunetti</i> , 139 S. Ct. 2294 (2019).....	17
<i>Landau v. CNA Fin. Corp.</i> , 886 N.E.2d 405 (Ill. App. 2008)	11
<i>Matsushita Elec. Indus. Co. v. Zenith Radio Corp.</i> , 475 U.S. 574 (1986).....	10
<i>Mazza v. Am. Honda Co., Inc.</i> , 666 F.3d 581 (9th Cir. 2012)	20
<i>McGoveran v. Amazon Web Services, Inc.</i> , 2021 WL 4502089 (D. Del. 2021)	<i>passim</i>

1	<i>Monroy v. Shutterfly</i> ,	
2	2017 WL 4099846 (N.D. Ill. 2017)	16
3	<i>Nat'l Collegiate Athletic Ass'n v. Miller</i> ,	
4	10 F.3d 633 (9th Cir. 1993), <i>overruled on other grounds by Olean Wholesale</i>	
5	<i>Grocery Coop., Inc. v. Bumble Bee Foods LLC</i> , 31 F.4th 651 (9th Cir. 2022)	20
6	<i>People v. Hanna</i> ,	
7	207 Ill. 2d 486 (2003)	23
8	<i>People v. Scheib</i> ,	
9	390 N.E.2d 872 (Ill. 1979)	17
10	<i>Reyn's Pasta Bella, LLC v. Visa USA, Inc.</i> ,	
11	442 F.3d 741 (9th Cir. 2006)	3
12	<i>Rivera v. Google</i> ,	
13	238 F. Supp. 3d 1088 (N.D. Ill. 2017)	16
14	<i>Rosenbach v. Six Flags Entertainment</i> ,	
15	129 N.E.3d 1197 (Ill. 2019)	21
16	<i>Sam Francis Found. v. Christies, Inc.</i> ,	
17	784 F.3d 1320 (9th Cir. 2015)	18
18	<i>Super Pawn Jewelry & Loan, LLC v. Am. Envtl. Energy, Inc.</i> ,	
19	2013 WL 1337303 (N.D. Ill. 2013)	15
20	<i>United States v. Pappadopoulos</i> ,	
21	64 F.3d 522 (9th Cir. 1995), <i>abrogated on other grounds by Jones v. United</i>	
22	<i>States</i> , 529 U.S. 848 (2000)	18
23	<i>Vulcan Golf, LLC v. Google Inc.</i> ,	
24	552 F. Supp. 2d 752 (N.D. Ill. 2008)	15
25	<i>Zellmer v. Facebook, Inc.</i> ,	
26	2022 WL 976981 (N.D. Cal. 2022)	<i>passim</i>
27	Statutes	
	740 ILCS 14/5(a)	22
	740 ILCS 14/5(b)	10, 22
	740 ILCS 14/10.....	13
	740 ILCS 14/15(b)	<i>passim</i>
	New York City Code § 22-1201	20

1	New York City Code § 22-1202	20
2	RCW 19.375.010	19
3	RCW 19.375.020	19
4	RCW 19.375.101(5).....	19
5	Other Authorities	
6	U.S. Constitution Commerce Clause	17
7	Fed. R. Civ. P. 56(a)	10
8	Creative Commons, About The Licenses, https://creativecommons.org/licenses/	
9	(last visited May 19, 2022)	3, 4
10	Flickr, How to Change Your License on Flickr https://www.flickrhelp.com/hc/en-	
11	us/articles/4404078674324-Change-Your-Photo-s-License-in-Flickr (last	
	visited May 19, 2022)	3
12	State of Delaware, Department of State: Division of Corporations, Business	
13	Search Results for Flickr Inc. and Yahoo, Inc.,	
14	https://icis.corp.delaware.gov/eCorp/EntitySearch/NameSearch.aspx (last	
	accessed May 19, 2022)	3

INTRODUCTION

In February 2019, Microsoft downloaded the IBM Diversity in Faces Dataset (“DiF Dataset” or “Dataset”), a collection of publicly available photos (and related data) from around the world that, without Microsoft’s knowledge, apparently contained links to photos of Illinois residents. Microsoft downloaded the Dataset from Washington and New York, quickly determined it was useless for Microsoft’s research purposes, and thus did not use it—for anything. This action presents the question whether Microsoft, a Washington-based company, can be held liable for statutory damages under the Illinois Biometric Information Privacy Act (“BIPA”), even though it took no action in Illinois and had no knowledge that any photos of or data regarding Illinois residents may have been in the Dataset. The answer is no. BIPA does not apply extraterritorially to Microsoft here because it engaged in no conduct that allegedly violated BIPA “primarily and substantially” in Illinois. To hold otherwise would violate the dormant Commerce Clause, as such a reading of BIPA would conflict with the Washington Biometric Privacy Law and New York law—the states in which Microsoft downloaded the Dataset. Further, BIPA cannot be read to require Microsoft to give prior notice and obtain consent merely to download the IBM-created Dataset when it has no relationship with and no practical means to contact the unknown individuals whose photos and information IBM included in the Dataset. Finally, having considered but never used the Dataset, Microsoft was not unjustly enriched by it.

The DiF Dataset is a large and diverse set of human faces that IBM, a New York company, created in New York to advance the study of fairness, accuracy, and bias in facial recognition technology. The Dataset contains links to roughly 1 million publicly available photos taken all over the world, as well as annotations of data regarding some (but not all) of the faces in the photos. In early 2019, IBM offered its DiF Dataset to approved researchers, free of charge, for use in research only. One Microsoft contractor and one Microsoft post-graduate student intern each downloaded the DiF Dataset, using an online link from IBM, from Washington and New York, respectively. Each did so to determine if the photos linked in the Dataset (not IBM’s annotations) would be useful in their research; each briefly evaluated some

1 of the linked photos; and each decided the Dataset didn't meet their respective research needs.
 2 Neither used IBM's DiF Dataset, nor did they share it with anyone else.

3 Illinois residents Steven Vance and Tim Janecyk now allege Microsoft (a) violated BIPA
 4 Section 15(b) simply by downloading the IBM DiF Dataset in Washington and New York
 5 without their consent—even though Microsoft could not have known their faces were in it; and
 6 (b) was unjustly enriched by downloading and profiting from use of Plaintiffs' biometric
 7 identifiers and information via the Dataset. The Court denied in part Microsoft's motion to
 8 dismiss, concluding "more factual refinement" about "the circumstances around Microsoft's
 9 attainment, possession and use of the Diversity in Faces dataset" was needed. Dkt. 43 at 8.
 10 Now, with the record developed, the Court should grant summary judgment for three reasons:

11 *First*, BIPA does not apply here because Microsoft did not engage in any action in
 12 Illinois, much less "primarily and substantially" in Illinois, as required for BIPA to govern.
 13 Microsoft did not download Plaintiffs' alleged biometrics in Illinois, did not use the Dataset or
 14 any information in Illinois (or anywhere), and did not have any reason to know the Dataset might
 15 contain links to Illinois residents' photos, much less their biometric identifiers. Further, if BIPA
 16 were construed to reach Microsoft's conduct in Washington and New York, the statute would
 17 violate the dormant Commerce Clause. In short, Microsoft cannot be liable for statutory
 18 damages based solely on incidental interaction with the DiF Dataset *entirely* outside Illinois.

19 *Second*, BIPA Section 15(b) does not require notice and consent before downloading a
 20 dataset of anonymous faces when, as here, a defendant has no relationship with the individuals
 21 depicted and no way of identifying them or finding out if they live in Illinois. "[I]t would be
 22 patently unreasonable to construe BIPA" to require notice to and consent from individuals who
 23 were "total strangers." *Zellmer v. Facebook, Inc.*, 2022 WL 976981, at *3 (N.D. Cal. 2022).

24 *Third*, even if the information in the DiF Dataset were biometric information or
 25 identifiers (a contested fact), Microsoft did not use that (or any other) information at all—so
 26 Plaintiffs have no unjust enrichment claim. Neither the contractor nor the intern reviewed or had
 27 any interest in the annotations in the Dataset, and neither shared the Dataset with anyone else.

Microsoft received no “benefit” or “profit” from Plaintiffs’ biometric information or identifiers.

UNDISPUTED MATERIAL FACTS

A. Flickr and the Yahoo-Created YFCC100M Dataset

Flickr is a photo sharing website that allows users to upload and share photos with others online. Compl. ¶ 28. Between at least 2004 and 2014, Flickr users could choose to upload their photos under either an “All Rights Reserved” license or a “Creative Commons” license.”¹ Under the former, the Flickr user retained the right to make copies and distribute uploaded photos. *Id.* Under the latter, the Flickr user consented to the ability of third parties to copy, distribute, edit, and use the photos.² The purpose of a Creative Commons license is to create a “digital commons, a pool of content that can be copied, distributed, edited, remixed, and built upon, all within the boundaries of copyright law.” *Id.*

In 2014, Yahoo!—Flickr’s then-parent³—publicly released a dataset of about 100 million photos uploaded to Flickr’s website between 2004 and 2014. Compl. ¶ 29; Dkt. 85 (“Merler Decl.”) at Ex. A (“IBM DiF Paper”). The dataset became known as the Yahoo Flickr Creative Commons 100 Million Dataset (YFCC100M), “the largest public multimedia collection that has ever been released, comprising a total of 100 million media objects [i.e., photos] . . . all of which have been uploaded to Flickr between 2004 and 2014 and published under a [Creative Commons] commercial or non-commercial license.” *Id.* at 66. The YFCC100M dataset includes only photos that users voluntarily allowed third parties to copy, distribute, and use. *Id.*

B. The IBM-Created DiF Dataset

In 2019, researchers at IBM released the DiF Dataset “to help advance the study of

¹ See Flickr, How to Change Your License on Flickr, <https://www.flickrhelp.com/hc/en-us/articles/4404078674324-Change-Your-Photo-s-License-in-Flickr> (last visited May 19, 2022) (describing the licenses supported by Flickr).

² Creative Commons, About The Licenses, <https://creativecommons.org/licenses/> (last visited May 19, 2022) (describing licenses as allowing “others [to] distribute, remix, adapt, and build upon your work”).

³ Both Flickr, Inc. and Yahoo Inc. are Delaware corporations based in California. See State of Delaware, Department of State: Division of Corporations, Business Search Results for Flickr Inc. and Yahoo, Inc., <https://icis.corp.delaware.gov/eCorp/EntitySearch/NameSearch.aspx> (last accessed May 19, 2022). The Court may take judicial notice of information on a state government website because it is “readily verifiable and, therefore, the proper subject of judicial notice.” *Reyn’s Pasta Bella, LLC v. Visa USA, Inc.*, 442 F.3d 741, 746, n.6 (9th Cir. 2006).

1 fairness and accuracy in face recognition technology.” IBM DiF Paper at 24. To create this
 2 dataset in compliance with “various copyright laws and privacy regulations,” IBM researchers
 3 used only photos from the YFCC100M dataset subject to the Creative Commons license. *Id.* at
 4 7-8. After selecting photos, IBM researchers applied 10 coding schemes and “annotations” from
 5 some of the photos in the dataset, including information related to some of the faces in some of
 6 the photos, such as “craniofacial distances” and “areas and ratios.” *Id.* at 9. They included other
 7 demographic information about some of the faces in the photos, such as the estimated age and
 8 gender. *Id.* at 9, 14–16. Information about faces in the photos linked in the DiF Dataset was
 9 “purely descriptive and designed to provide a mechanism to evaluate diversity in the dataset—
 10 not to provide a method of facial identification.” Merler Decl. ¶ 7.

11 IBM researchers who created the DiF Dataset did so in New York, and IBM created and
 12 stored the Dataset on servers in New York. *Id.* at ¶ 8. IBM did not create the Dataset in Illinois,
 13 did not store it on computers in Illinois, and did not take any other actions involving the Dataset
 14 in Illinois. *Id.* The Dataset Terms of Use prohibited recipients of the Dataset from “attempt[ing]
 15 to identify any individuals within the IBM Research DiF Dataset.” Merler Decl., Ex. H, Terms
 16 of Use at 3. IBM made the DiF Dataset available for free download to researchers who filled out
 17 a questionnaire certifying that they sought access for research purposes only. Merler Decl. ¶ 9.

18 **C. Plaintiffs’ Flickr Photos**

19 Plaintiffs assert that, while in Illinois, they uploaded photos of themselves and others to
 20 their Flickr accounts. Compl. ¶¶ 60, 69; Dkt. 86 (“Berger Decl.”) Ex. 1 (“Vance Dep.”) 132:4–6;
 21 *id.* Ex. 2 (“Janecyk Dep.”) 99:21–100:13. When signing up for Flickr, Plaintiffs did not exercise
 22 the option to restrict who could access their photos, such as choosing the All Rights Reserved
 23 license. Vance Dep. 207:17–208:4; Janecyk Dep. 72:2–24. Instead, they uploaded their photos
 24 under the Creative Commons license, Vance Dep. 206:1–6; Janecyk Dep. 72:2–9, granting the
 25 public “license” to “distribute, remix, adapt, and build upon [their] work[.]” Creative Commons,
 26 About The Licenses, <https://creativecommons.org/licenses/> (last visited May 19, 2022).

27 Vance testified that he uploaded at least 18,595 public photos to Flickr, and at least 63 of

1 these were included by IBM in the DiF Dataset. Vance Dep. 179:22–23; 210:19–24. These 63
 2 photos depict other people, not just Vance, and he did not always know whether these people were
 3 Illinois residents. *Id.* at 132:4–14; 154:5–16. Some of these 63 photos were taken by someone
 4 other than Vance, and some were taken outside Illinois. *Id.* at 70:2–71:22; 131:10–132:2.

5 Janecyk uploaded 1,669 public photos to Flickr, 24 of which became part of the Dataset.
 6 Janecyk Dep. 74:21–24; 95:22–96:1. Janecyk’s practice was to photograph strangers on the streets
 7 of Chicago. *Id.* 45:16–46:19. Aside from himself and people Janecyk knew only as “Popcorn
 8 Mike” and “Dave,” Janecyk did not know the names of *anyone* in the 24 photos and did not know
 9 where they lived. *Id.* 98:8–100:13; 167:11–168:15; 225:9–227:4; 228:19–21. At least two of the
 10 24 photos were taken outside of Illinois. *Id.* 97:18–20. Janecyk put a note on his account saying
 11 “PLEASE STEAL MY PHOTOS! ... I encourage you to steal any of my photography for
 12 personal or commercial use.” Berger Decl. Ex. 3; Janecyk Dep. Ex. 4; *id.* 88:14–89:6.

13 Neither Vance nor Janecyk alleges he had any contact or communication with Microsoft
 14 (in Illinois or elsewhere) concerning the DiF Dataset or their photos on Flickr. Vance Dep. 187:9–
 15 19; 199:13–16; Janecyk Dep. 95:3–6. Neither Plaintiff contacted IBM about removing their photos
 16 from the Dataset upon learning they were in it. *Id.*

17 **D. Microsoft Contractor Benjamin Skrainka’s Download of the DiF Dataset**

18 In early 2019, Benjamin Skrainka was an independent contractor working for Neal
 19 Analytics LLC, a Washington-based consulting firm that supports companies with their data-
 20 driven initiatives. Dkt. 87 (“Skrainka Decl.”) ¶ 2; Skrainka Dep. 91:15-20.⁴ Through Neal
 21 Analytics, Skrainka worked as a vendor to Microsoft from September 7, 2018, through August 1,
 22 2019. Skrainka Decl. ¶ 2; Skrainka Dep. 91:21-24. In that role, Skrainka provided support for a
 23 project where he applied industry standard benchmarks to evaluate facial recognition technology.
 24 Skrainka Decl. ¶ 3; Skrainka Dep. 127:7-16. He determined what the parameters and/or
 25 methodology should be for comparing different face recognition technologies available in the
 26 _____

27 ⁴ Other than excerpts from Plaintiffs’ depositions (attached as exhibits to Dkt. 86), all other deposition excerpts are
 attached to the concurrently-filed Wiese Declaration.

1 market. Skrainka Decl. ¶ 3; Skrainka Dep. 126:18-127:10; Dkt. 91 (“Kasap Decl.”) ¶ 4.

2 As part of his work, Skrainka sought datasets containing photos suitable for his project.
 3 Skrainka Decl. ¶ 4; Skrainka Dep. 139:4-140:24. Around February 1, 2019, Skrainka, while
 4 working in Washington, filled out an IBM questionnaire requesting a copy of the DiF Dataset for
 5 use in his project. Skrainka Decl. ¶¶ 4–5; Skrainka Dep. 198:14-199:10. After IBM granted
 6 Skrainka access through an online link, he downloaded the Dataset in February 2019. Skrainka
 7 Decl. ¶ 5; Skrainka Dep. 217:1-219:14. Skrainka was in Washington when he downloaded the
 8 DiF Dataset. Skrainka Decl. ¶ 5; Skrainka Dep. 217:1-219:14; 371:22-372:9.

9 Skrainka obtained the DiF Dataset solely to evaluate whether the photos linked in it were
 10 useable in his project. Skrainka Decl. ¶ 6; Skrainka Dep. 233:7-234:5. He was not interested in
 11 any facial annotations or any other data that IBM may have included in its DiF Dataset, and he
 12 never reviewed any such data. Skrainka Decl. ¶ 6; Skrainka Dep. 208:3-15, 227:21-229:23,
 13 373:11-20. As it turned out, the linked photos in the Dataset were useless for Skrainka’s
 14 research because they were unconstrained images, i.e., they were not conventional head-on
 15 photos used on a driver’s license or passport, and they were of generally low quality. Skrainka
 16 Decl. ¶ 7; Skrainka Dep. 233:24-235:6.

17 Once Skrainka determined the photos were useless, he spent no more time with the DiF
 18 Dataset. Skrainka Decl. ¶ 7; Skrainka Dep. 246:16-23, 251:12-23. He did not share the link to
 19 or the Dataset itself with anyone. Skrainka Decl. ¶ 5; Skrainka Dep. 223:1-3. Because he was
 20 focused on locating suitable photos, Skrainka ignored—and was not even aware of—other data
 21 IBM may have included in the DiF Dataset; nor did he know the Dataset included data relating to
 22 some Illinois residents. Skrainka Decl. ¶¶ 6-10; Skrainka Dep. 358:17-23. (Skrainka did,
 23 however, review some limited metadata included in the DiF Dataset. *Id.* 226:6-9; 229: 24-
 24 230:21.) Neither Skrainka nor Mustafa Kasap, the Microsoft Principal Program Manager
 25 supervising Skrainka’s work for Azure Media Services (f/k/a Azure Intelligent Storage), are
 26 aware of anyone at Microsoft using or accessing the DiF Dataset in any project or product at
 27 Microsoft. Skrainka Decl. ¶ 12; Skrainka Dep. 220:1-3; Kasap Decl. ¶ 7; Kasap Dep. 55:12-20.

1 Skrainka does not recall exactly where he saved his copy of the DiF Dataset. Skrainka
 2 Decl. ¶ 8. But he does recall that “any facial-recognition-related work that [he] performed . . .
 3 was loaded only onto virtual machines and cloud storage in Azure.”⁵ Skrainka Dep. 188:12-23.
 4 In setting up the virtual machines and blob storage in Azure, Skrainka would have “provision[ed]
 5 [the] machine[] in a specific availability zone.” *Id.* at 149:8-15. The selection of an Azure
 6 Region determines the geography of the data centers where the data will be stored. Kuttiyan
 7 Decl. ¶ 3. Within each Azure Region, Microsoft has availability zones that map to specific data
 8 centers within the selected region. *Id.* Skrainka said he used “a West Coast availability zone”
 9 for the work he performed for Azure Media Services, Skrainka Dep. 147:2-6, and that “it’s
 10 almost surely the case that we were using West Coast data centers” for his project, given “a bias
 11 for using West Coast data centers because they’re faster,” *id.* at 154:10-20. In February 2019,
 12 data stored in virtual machines or blob storage in an Azure Region corresponding with the “West
 13 US” or “West US 2” Azure Regions would have been stored in data centers in either Washington
 14 or California—not in Illinois. Kuttiyan Decl. ¶ 4 & Ex. A.

15 Despite a reasonable investigation, Microsoft has been unable to confirm if and where
 16 Skrainka stored his downloaded copy of the DiF Dataset. *See* Kasap Decl. ¶ 6; Dkt. 92
 17 (“Bruncke Decl.”) ¶¶ 5–6; Bruncke Dep. 63:10-64:6, 96:10-12, 99:15-105:18. Andy Bruncke, a
 18 Senior Program Manager at Microsoft who oversaw the relationship with Neal Analytics,
 19 searched for any record of Skrainka’s downloaded copy of the DiF Dataset in the locations
 20 where vendors and Microsoft employees stored data for the relevant research project. Bruncke
 21 Decl. ¶ 6; Bruncke Dep. 99:15-105:18. Bruncke did not locate either a copy of the DiF Dataset
 22 or a record of it ever having been stored in those locations. Bruncke Decl. ¶ 6; Bruncke Dep.
 23 96:10-12, 99:15-105:18. Skrainka used his own Apple laptop for his work—not any Microsoft-
 24 issued device for his work related to the DiF Dataset. Skrainka Decl. ¶ 9; Skrainka Dep. 150:21-

25
 26
 27 ⁵ A virtual machine emulates the characteristics of a stand-alone physical computer. Skrainka Decl. ¶ 8. It shares physical resources, such as servers, with other virtual machines, and each virtual machine is isolated by software. *Id.* A virtual machine can easily be created, modified, or decommissioned without affecting the host computer. *Id.*

151:6. When his project ended in approximately August 2019, Skrainka decommissioned all the virtual machines he used on the project and deleted from his own computer all resources he used during the project, including any datasets. Skrainka Decl. ¶¶ 8-9; Skrainka Dep. 253:20-23.

E. Microsoft Student Intern Samira Samadi's Download of the DiF Dataset

In February 2019, Samira Samadi, a graduate student at Georgia Institute of Technology, worked as a student intern at Microsoft Research's New York City office. Dkt. 88 ("Samadi Decl.") ¶ 2. Samadi downloaded the DiF Dataset for a research project overseen by Jenn Wortman Vaughan, a Microsoft Senior Principal Researcher. Samadi Decl. ¶¶ 5-6; Dkt. 89 ("Vaughan Decl.") ¶ 3, 5; Vaughan Dep. 27:12-28:3. Samadi's internship research project involved the study of how humans interact with, use, and make decisions with facial recognition systems. Samadi Decl. ¶ 3. She wanted to design a controlled human-subject experiment where participants were shown examples of images of faces deemed similar by an automatic facial recognition system and then were asked to judge the similarities of the faces in the images. *Id.* The goal of Samadi's research was to measure how the perceived race, skin tone, and gender of the faces affect human judgment of face similarities. *Id.*

After reading about the DiF Dataset, Samadi thought it might be a useful resource, as the photos linked in the Dataset apparently had been selected to represent a diverse demographic cross-section. *Id.* at ¶ 5. From New York, and using her Georgia Institute of Technology email address, Samadi emailed IBM on February 20, 2019, requesting access to the IBM DiF Dataset. *Id.*; Samadi Dep. 204:1-6. After she filled out a questionnaire, she was granted access to the DiF Dataset via an online link. Samadi Decl. ¶ 6; Samadi Dep. 74:1-21. Samadi downloaded the Dataset from IBM on or about February 25, 2019, in New York City. Samadi Decl. ¶ 6.

Once Samadi did so, she reviewed some of the photos linked in the DiF Dataset and quickly determined they were unsuitable for her research. Samadi Decl. ¶ 7; Samadi Dep. 51:18-52:5. The Dataset did not contain multiple photos of the same individual facing the camera, which was necessary to simulate the hypothetical facial recognition system her research required. Samadi Decl. ¶ 7; Samadi Dep. 77:13-19. After Samadi made that determination, she

1 did not review any other data in the DiF Dataset. Samadi Decl. at ¶ 8; Samadi Dep. 177:15-
 2 178:1. Neither Samadi nor her supervisor Vaughan used the Dataset in their research projects.
 3 Samadi Decl. ¶ 7; Samadi Dep. 51:18-52:5; Vaughan Decl. ¶ 10; Vaughan Dep. 45:13-22.
 4 Further, Samadi did not share the link to or the Dataset itself with anyone. Samadi Decl. ¶ 8;
 5 Samadi Dep. 155:19-21, 208:16-209:3. When Samadi downloaded it, she did not know the
 6 Dataset included any facial measurements or other similar data added by IBM, nor did she know
 7 the Dataset included Illinois residents' data. Samadi Decl. ¶¶ 8-9; Samadi Dep. 177:15-178:1.

8 Samadi does not recall where she saved the copy of the DiF Dataset, but she believes she
 9 likely downloaded it to a laptop Microsoft issued for her internship. Samadi Decl. ¶ 6; Samadi
 10 Dep. 31:8-20, 32:15-33:1, 57:11-19, 63:18-64:3, 199:6-16; Wiese Decl., Ex. 8, at Second Supp.
 11 Response No. 8. Based on Microsoft's Data Retention and Disposal Standard, data on Samadi's
 12 Microsoft-issued laptop was deleted within 180 days of the end of her internship (i.e., by October
 13 30, 2019). *See* Dkt. 90 ("Swann Decl.") ¶ 9; Swann Dep. 197:21-198:12. But Microsoft found a
 14 copy of the DiF Dataset that Samadi downloaded, along with other data from Samadi's
 15 internship, on a Microsoft Research server in New York. *See* Dkt. 93 ("Chirico Decl.") ¶ 3 &
 16 Ex. B. The server is physically located in New York. *Id.* at ¶ 3. There are no servers hosting
 17 backups of the New York server, and access to the New York server is restricted to Microsoft
 18 Research. *Id.*; Chirico Dep. 44:24-46:9. The DiF Dataset was saved in a "hidden share,"
 19 meaning that even a Microsoft Research team member could not access it unless she knew the
 20 specific file path. Chirico Decl. ¶ 3; Chirico Dep. 53:21-54:8.

21 Microsoft has searched for but found no evidence to suggest the copy of the DiF Dataset
 22 that Samadi downloaded was ever downloaded to or stored on any Microsoft storage device or
 23 equipment, including servers, other than the local New York server physically located in New
 24 York or Samadi's Microsoft-issued laptop. Neither Samadi nor Vaughan is aware of anyone at
 25 Microsoft using or accessing the DiF Dataset in any project or product at Microsoft, other than
 26 Samadi's brief evaluation of some photos in and rejection of the Dataset. Samadi Decl. ¶ 12;
 27 Samadi Dep. 260:20-261:15; Vaughan Decl. ¶ 10-11; Vaughan Dep. 124:20-125:4.

1 Plaintiffs seek damages on their BIPA Section 15(b) and unjust enrichment claims.

2 ARGUMENT

3 The Court should grant summary judgment “if the movant shows that there is no genuine
4 dispute as to any material fact and the movant is entitled to a judgment as a matter of law.” Fed.
5 R. Civ. P. 56(a). To avoid summary judgment, the nonmovant must come forward with “specific
6 facts showing that there is a *genuine issue for trial*.” *Matsushita Elec. Indus. Co. v. Zenith Radio*
7 *Corp.*, 475 U.S. 574, 587 (1986); *see also Hesketh v. Total Renal Care, Inc.*, 2021 WL 5761610,
8 at *7 (W.D. Wash. 2021) (Robart, J.). Because Microsoft “does not bear the ultimate burden of
9 persuasion at trial,” it is entitled to judgment “by showing that the nonmoving party lacks
10 evidence of an essential element of its claim[.]” *Hesketh*, 2021 WL 5761610, at *7.

11 **I. BIPA Does Not and Cannot Constitutionally Apply to Microsoft’s Activities in** 12 **Washington and New York.**

13 The two people associated with Microsoft who briefly interacted with some photos in the
14 DiF Dataset in Washington and New York did not know it might have contained links to photos
15 or data of Illinois residents, nor did they use the Dataset for any purpose. Plaintiffs nevertheless
16 assert that Microsoft should be subject to statutory damages under BIPA for failing to obtain
17 their consent before downloading the DiF Dataset outside Illinois. Such an interpretation of
18 BIPA would lead to absurd consequences, imposing statutory damages on private entities for
19 unknowingly coming into possession of data allegedly about Illinois residents, but taking no
20 actions in Illinois and never using that data. Nothing in BIPA suggests the statute was intended
21 to have extraterritorial effect. To the contrary, the Illinois General Assembly’s findings show it
22 was concerned with companies coming *into* Illinois and collecting Illinois residents’ biometrics.
23 *See* 740 ILCS 14/5(b). As a matter of Illinois law, BIPA does not apply to Microsoft’s out-of-
24 state conduct. Further, its application here would violate the dormant Commerce Clause.

25 **A. BIPA Does Not Apply Extraterritorially to Microsoft.**

26 As this Court has acknowledged, BIPA “is not authorized to have extraterritorial effect”
27 as a matter of Illinois law. Dkt. 43 at 6. To establish a BIPA claim, Plaintiffs must prove

Microsoft violated the statute and that its violation “occur[red] primarily and substantially in Illinois.” *Id.* (quoting *Avery v. State Farm Mutual Auto. Ins. Co.*, 835 N.E.2d 801, 854 (Ill. 2005)). Put another way, Microsoft could be subject to BIPA only if “the majority of circumstances relating to the alleged violation” occurred in Illinois. *Landau v. CNA Fin. Corp.*, 886 N.E.2d 405, 409 (Ill. App. 2008). Another district court recently dismissed a BIPA putative class action because, like here, a plaintiff sought to apply the statute improperly to conduct that did not occur “primarily and substantially” in Illinois. *See McGoveran v. Amazon Web Services, Inc.*, 2021 WL 4502089, at *6 (D. Del. 2021). This Court should reach the same conclusion.

1. The Undisputed Facts Confirm Microsoft’s Relevant Conduct Occurred Entirely Outside Illinois.

BIPA Section 15(b) prohibits any “private entity” from obtaining any person’s biometrics without first giving notice and obtaining consent. 740 ILCS 14/15(b). Plaintiffs claim Microsoft violated Section 15(b) of BIPA because it allegedly downloaded a dataset that contained their biometrics without first receiving their written consent or telling them the purpose and duration of Microsoft’s collection. The relevant conduct underlying Plaintiffs’ BIPA claim involves a Microsoft contractor in Washington and a Microsoft student intern in New York. These two individuals each downloaded the DiF Dataset, briefly evaluated some photos linked in the Dataset, and then rejected the Dataset for use in research projects in Washington and New York. Skrainka Decl. ¶ 7; Skrainka Dep. 251:12-23; Samadi Decl. ¶ 7; Samadi Dep. 51:18-52:5. Neither the contractor nor the intern used the DiF Dataset; neither shared the Dataset with anyone else; and neither is aware of anyone else at Microsoft using it. Skrainka Decl. ¶¶ 7, 12; Skrainka Dep. 220:1-3; Samadi Decl. ¶¶ 7, 8, 12; Samadi Dep. 260:20-261:15. As this Court emphasized in its order on Microsoft’s motion to dismiss, the only question is “whether and to what extent Microsoft’s alleged acts involving the Diversity in Faces dataset occurred in Illinois.” Dkt. 43 at 10. The answer: not at all.

Far from showing any connection to Illinois, the evidence shows that Microsoft’s conduct was several steps *removed* from Illinois. The DiF Dataset, which allegedly included facial

1 annotations from publicly available photos taken and uploaded from around the world, was
 2 created by IBM in New York. Merler Decl. ¶ 8. IBM used the YFCC100M dataset created by
 3 Yahoo! and Flickr, which are both Delaware corporations based in California. Skrainka and
 4 Samadi each downloaded and briefly evaluated some photos linked in the DiF Dataset while in
 5 Washington and New York, respectively. Skrainka Decl. ¶¶ 5, 7; Skrainka Dep. 371:22-372:9;
 6 Samadi Decl. ¶ 7; Samadi Dep. 51:18-52:5. And that is all either did.

7 Skrainka did not use a Microsoft-issued laptop for his project, does not recall where he
 8 saved his copy of the DiF Dataset, and deleted all resources he used in the project, including any
 9 stored data, when his project ended in about August 2019. Skrainka Decl. ¶¶ 8-9; Skrainka Dep.
 10 150:21-151:6. To the extent he saved the Dataset to the virtual machine or blob storage he
 11 created for his work, the Dataset would have been stored in data centers in California or
 12 Washington. *See* Skrainka Dep. 188:12-23, 149:8-15; Kuttiyan Decl. ¶ 3. And the copy of the
 13 DiF Dataset downloaded by Samadi was stored on her Microsoft-issued laptop, as well as a
 14 Microsoft Research local server physically located in New York and not backed up anywhere
 15 else. Samadi Dep. 31:8-20, 32:15-33:1; Chirico Decl. ¶ 3; Chirico Dep. 44:24-46:9.

16 During their work at Microsoft, Skrainka and Samadi both had access to Microsoft's
 17 cloud file hosting and storage service, OneDrive for Business ("OneDrive"). Swann Decl. ¶ 4;
 18 Swann Dep. 160:2-8. Microsoft, like many businesses, has a OneDrive subscription, which
 19 allows its employees and vendors to store files and data in the cloud. *Id.* But Microsoft has no
 20 reason to believe Skrainka or Samadi ever saved a copy of the Dataset to OneDrive. *Id.* at ¶ 5;
 21 Swann Dep. 153:19-154:21. Skrainka testified that he saved the Dataset to either a virtual
 22 machine or blob storage—not to OneDrive. Skrainka Dep. 178:20-179:12, 220:9-12. And the
 23 Azure Region chosen when setting up a virtual machine or blob storage is independent of the
 24 storage location for any data that a user might save to OneDrive. Kuttiyan Decl. ¶ 5.

25 Microsoft has no reason to believe the DiF Dataset was ever saved to OneDrive, and
 26 there is no evidence it was. Swann Decl. ¶ 5; Skrainka Dep. 147:2-6; Kuttiyan Decl. ¶ 4; Chirico
 27 Decl. ¶ 3; Samadi Decl. ¶ 5; Samadi Dep. 57:11-19, 63:18-64:3, 199:6-16; Wiese Decl., Ex. 8, at

1 Second Supp. Response to Interrogatory No. 8. Plaintiffs may argue otherwise, but they may not
 2 rely on hypotheticals or “unsupported conjecture” to resist summary judgment. *See, e.g.,*
 3 *Hernandez v. Spacelabs Med. Inc.*, 343 F.3d 1107, 1112 (9th Cir. 2003). The storage location
 4 for data saved to OneDrive thus has no bearing on this motion.

5 But even if, hypothetically, Skrainka or Samadi *had* saved the DiF Dataset file to
 6 OneDrive, that would make no difference. Had they done so, the file would have been chunked
 7 (i.e., divided into non-overlapping packets of data bits, roughly one megabyte in size) and
 8 encrypted; these chunks “would have been inaccessible and unintelligible without decryption and
 9 reassembly.” Swann Decl. ¶ 4; Swann Dep. 63:4-16. The encrypted chunks, if any, would have
 10 then been stored in data centers, likely in San Antonio, Texas, and/or Chicago, Illinois. Swann
 11 Decl. ¶ 4; Swann Dep. 69:9-70:4; 71:4-21; 81:4-14; 84:2-8, 165:14-20, 166:6-9. Even if any
 12 encrypted chunks of the Dataset had been stored in Illinois at some point (a pure hypothetical
 13 that Microsoft disputes), that has nothing to do with violating BIPA: Section 15(b) regulates
 14 only *acquisition* of data through conduct primarily and substantially in Illinois, not encrypted
 15 *storage* of fragmented data after acquisition. *See* 740 ILCS 14/15(b). The totality of Microsoft’s
 16 relevant conduct occurred entirely outside of Illinois.

17 The evidence confirms the scenario this Court recognized in ruling on Microsoft’s motion
 18 to dismiss, i.e., “[i]t is certainly possible with more factual refinement around this complex issue,
 19 the circumstances around Microsoft’s attainment, possession and use of the Diversity in Faces
 20 dataset will reveal that the alleged violations did not occur primarily in Illinois.” Dkt. 43 at 8.

21 **2. Microsoft’s Alleged BIPA Violation Had No Connection to Illinois.**

22 Because Microsoft did nothing in Illinois relating to the DiF Dataset, Plaintiffs attempt to
 23 support the application of BIPA here by alleging they uploaded photos to Flickr while in Illinois
 24 many years before IBM created its Dataset. But Microsoft did not allegedly violate Section
 25 15(b) when Plaintiffs uploaded their photos. For one thing, BIPA exempts “photographs” from
 26 its definition of “biometric identifier,” so there is no BIPA significance to Plaintiffs simply
 27 uploading their photos. 740 ILCS 14/10. Further, Microsoft allegedly violated BIPA not when

1 Plaintiffs uploaded their photos, but years later, when Skrainka and Samadi clicked links from
 2 Washington and New York to download IBM's New York-created DiF Dataset, which allegedly
 3 contained Plaintiffs' biometrics. As the Court recognized, the relevant inquiry on Plaintiffs'
 4 BIPA claim is "whether and to what extent Microsoft's alleged acts involving the Diversity in
 5 Faces dataset occurred in Illinois." Dkt. 43 at 10. The evidence shows Microsoft's conduct did
 6 not occur in Illinois at all.

7 In analyzing the motion to dismiss on extraterritoriality, this Court noted that if Microsoft
 8 had made disclosures to or sought consent from Illinois residents, "any communication would
 9 have necessarily involved Illinois." Dkt. 43 at 8. But Microsoft did *not* communicate with
 10 Illinois residents (or residents of other states) whose photos were linked in the DiF Dataset.
 11 Indeed, the two people associated with Microsoft who downloaded the Dataset were not even
 12 aware it might contain links to photos or annotations from Illinois residents. Skrainka Decl. ¶
 13 10; Skrainka Dep. 358:17-23; Samadi Decl. ¶ 9; Samadi Dep. 257:1-5. The absence of any
 14 communications with Illinois residents confirms that the circumstances giving rise to Plaintiffs'
 15 claims did not occur primarily and substantially in Illinois. To hold otherwise would make BIPA
 16 apply to anyone who obtains an Illinois resident's biometric data, even unwittingly, without
 17 regard to where the defendant resides or engaged in the activities giving rise to the claim.
 18 Further, the *absence* of communications in Illinois cannot bring otherwise extraterritorial events
 19 within BIPA's reach—because, as a logical matter, the *absence* of conduct cannot be conduct
 20 occurring "primarily and substantially" in Illinois.

21 The court in *McGoveran v. Amazon Web Services, Inc.*, made this point when granting
 22 the defendants' motion to dismiss a BIPA case for lack of extraterritorial application. *See* 2021
 23 WL 4502089, at *6. There, the plaintiffs argued that the defendants "failed to make written
 24 biometric data retention and destruction policies available to the public and that they failed to
 25 provide notice to and obtain consent from Illinois citizens." *Id.* at *4. But the court rejected the
 26 notion that a location could be assigned for an alleged failure to act:

27 The Court does not see why that must be true. (*See* Tr. at 10) ("It really makes no
 sense to assign a location for an act that did not occur.") More fundamentally, that

argument depends on the assumption that Defendants were required to provide notice, publish policies, and obtain consent in Illinois. . . . Plaintiffs have not alleged any activity in Illinois that would impose such obligations on Defendants.

Id. See *David K. Lindemuth Co. v. Shannon Fin. Corp.*, 637 F. Supp. 991, 994 (N.D. Cal. 1986) (“[t]here is no ‘place’ where [an] omission occur[s]”).

The absence of any harm to Plaintiffs in Illinois further demonstrates that Microsoft’s conduct had no connection to Illinois. The uncontroverted evidence shows that contrary to Plaintiffs’ allegations, there is no “ongoing” harm to privacy interests for Illinois residents. Compl. ¶¶ 67,75, 77. Two people affiliated with Microsoft briefly looked at some photos linked in the Dataset (but none of IBM’s data or annotations), quickly determined the Dataset was unsuitable, and did not use or share it with anyone else at Microsoft. And the evidence shows no one else at Microsoft used the DiF Dataset either. Kasap Decl. ¶¶ 7-8; Bruncke Decl. ¶ 7; Bruncke Dep. 64:7-19; Vaughan Decl. ¶ 11; Vaughan Dep. 124:20-125:4; Samadi Decl. ¶ 12; Skrainka Decl. ¶ 12. The evidence establishes no harm to Illinois residents, much less ongoing harm, by Microsoft’s download and brief review of some photos contained in the Dataset.

The information that Plaintiffs allege was protected by BIPA was created by IBM in New York, not Illinois, several years after Plaintiffs uploaded photos from which their alleged biometrics were derived. Microsoft’s alleged conduct with respect to the DiF Dataset containing that information occurred in Washington and New York, not Illinois. Because BIPA has no extraterritorial effect and Microsoft’s conduct occurred entirely outside Illinois, BIPA does not apply to Microsoft here, and the Court should grant summary judgment.

3. Plaintiffs’ Illinois Residency Alone Cannot Satisfy Illinois’ Extraterritoriality Doctrine.

The only connection between Plaintiffs’ BIPA claim and Illinois is that they are Illinois residents who assert they uploaded photos to Flickr while in Illinois. Compl. ¶¶ 6-7, 60-61, 69. That does not suffice for the application of BIPA. Plaintiffs’ residence alone cannot satisfy Illinois’ requirement that *Microsoft’s* alleged violation of BIPA must have occurred primarily and substantially in Illinois. See, e.g., *Super Pawn Jewelry & Loan, LLC v. Am. Envtl. Energy*,

1 *Inc.*, 2013 WL 1337303, at *7 (N.D. Ill. 2013) (no substantial connection though plaintiff was an
 2 Illinois business); *Vulcan Golf, LLC v. Google Inc.*, 552 F. Supp. 2d 752, 775 (N.D. Ill. 2008)
 3 (dismissing case when only contact was plaintiffs' Illinois residency).

4 In *McGoveran*, the court refused a similar attempt to apply BIPA extraterritorially based
 5 solely on the plaintiffs' Illinois residence. *See* 2021 WL 4502089, at *6. There, plaintiffs
 6 alleged that when they called a call center located in Massachusetts, one defendant, who was
 7 based in Georgia and provided voice technology to the company that operated the call center,
 8 "extracted biometric information from calls originating from Illinois, from Illinois citizens, and
 9 from clearly recognizable Illinois phone numbers," and one defendant, who was based in
 10 Washington "intercepted biometric information" from Illinois callers. *Id.* at *4. The plaintiffs
 11 argued BIPA applied to this conduct because they were in Illinois when they called
 12 Massachusetts. *Id.* According to them, "under BIPA, as long as the source of the biometric data
 13 is Illinois, that's enough to establish liability." *Id.* at *6.

14 The district court flatly rejected this argument. "There is no basis in the statutory
 15 language to find that BIPA stretches so far." *Id.* The court held "[t]he location of the caller does
 16 not . . . say anything about the location where the rest of the conduct occurred," and there was no
 17 indication in the complaint that the non-Illinois defendants "did anything in Illinois." *Id.* at *4.
 18 Because the defendants did not do "anything" in Illinois, it followed that any BIPA violations did
 19 not occur "primarily and substantially" in Illinois. *Id.* at *6. The court distinguished decisions
 20 denying motions to dismiss (not summary judgment motions) in *Rivera v. Google*, 238 F. Supp.
 21 3d 1088 (N.D. Ill. 2017), and *Monroy v. Shutterfly*, 2017 WL 4099846 (N.D. Ill. 2017), noting
 22 that in both those cases the defendants were alleged to have directly and intentionally interacted
 23 with the plaintiffs in Illinois. *Id.* at *5-6.

24 This case is analogous to *McGoveran*. Microsoft had no interaction with Plaintiffs, and
 25 its conduct cannot be fairly attributed to Illinois. Nothing happened in Illinois other than
 26 Plaintiffs allegedly uploading their photos to Flickr in Illinois, years before IBM created its DiF
 27 Dataset in New York. Vance Dep. 187:9–19; 199:13–16; Janecyk Dep. 95:3–6. That is the *only*

conceivable connection between Plaintiffs’ claims and Illinois.⁶ Plaintiffs ask the Court to adopt the very rule for which the *McGoveran* court found “no basis”: that a plaintiff’s location in Illinois is enough to implicate BIPA even when the conduct forming the alleged BIPA violation occurred entirely outside Illinois. As the *McGoveran* court rightly acknowledged, that outcome makes no sense, as it would mean “BIPA could impose liability on a vast number of corporations who do no business in Illinois and who lack any other significant connection to Illinois.” *McGoveran*, 2021 WL 4502089, at *6. Nothing in the Illinois legislative history or findings for BIPA suggests the legislature intended for BIPA to have such sweeping effect. The Court should follow *McGoveran* and reject Plaintiffs’ Section 15(b) claim.

B. Applying BIPA to Microsoft’s Out-of-State Conduct Would Violate the Dormant Commerce Clause.

Illinois courts “do not favor any [statutory] construction that would raise legitimate doubts as to the constitutional validity of a statutory provision.” *People v. Scheib*, 390 N.E.2d 872, 876 (Ill. 1979); accord *Iancu v. Brunetti*, 139 S. Ct. 2294, 2301 (2019). But if BIPA were construed to apply to Microsoft here (and it should not be), the dormant Commerce Clause would prohibit its use to impose liability on Microsoft for its extraterritorial conduct.

The Commerce Clause of the U.S. Constitution, Article I, section 8, has long been understood to have a negative implication “commonly known as the dormant Commerce Clause.” *Daniels Sharpsmart, Inc. v. Smith*, 889 F.3d 608, 614 (9th Cir. 2018). The dormant Commerce Clause prohibits a state from “directly affect[ing] transactions that take place across state lines or entirely outside of the state’s borders.” *Id.* at 614–15 (quoting *S.D. Myers, Inc. v. City & County of San Francisco*, 253 F.3d 461, 467 (9th Cir. 2001)). If a state statute directly regulates conduct entirely outside of the state’s borders, the statute is “struck down . . . without

⁶ In *McGoveran*, the court acknowledged the Washington-based company’s data centers “are located wholly outside Illinois – in Virginia, Ohio, California, and Oregon.” 2021 WL 4502089, at *4. Although Microsoft does have an Illinois data center, no evidence shows the DiF Dataset was ever stored there (*see supra* at 12-13), and unlike in *McGoveran*, this case is presented on summary judgment, where Plaintiffs have the burden of presenting evidence. In any event, as explained above, the merely hypothetical, transitory storage of encrypted chunks of data cannot give rise to liability under Section 15(b).

1 further inquiry.” *Chinatown Neighborhood Ass’n v. Harris*, 794 F.3d 1136, 1145 (9th Cir. 2015)
 2 (citation omitted). In addition, the dormant Commerce Clause prevents “inconsistent legislation
 3 arising from the projection of one state regulatory regime into the jurisdiction of another
 4 State.” *Healy v. Beer Institute, Inc.*, 491 U.S. 324, 337 (1989) (citation omitted). This case
 5 presents both dormant Commerce Clause scenarios, although each is independently sufficient.
 6 *Id.* at 336–37 (the Commerce Clause protects both against inconsistent legislation “generally” or
 7 against one state “specifically ... forc[ing] an out-of-state merchant to seek regulatory approval
 8 in one State before undertaking a transaction in another”).

9 **1. Plaintiffs May Not Use BIPA to Regulate Conduct Occurring Outside**
 10 **Illinois’ Borders.**

11 “Congress’s power to regulate articles or goods in commerce may not permit it to
 12 regulate an item for eternity simply because it has once passed state lines.” *United States v.*
 13 *Pappadopoulos*, 64 F.3d 522, 527 (9th Cir. 1995), *abrogated on other grounds by Jones v.*
 14 *United States*, 529 U.S. 848, 854 (2000). So, too, Illinois may not regulate a photo (or
 15 information derived from a photo) anywhere in the world simply because it was taken in Illinois
 16 or contains information about an Illinois resident. For example, in *Daniels Sharpsmart*, the
 17 Ninth Circuit held a party would likely succeed on its claim that California violated the dormant
 18 Commerce Clause when it attempted to regulate how medical waste created in California could
 19 be disposed of elsewhere. 889 F.3d at 616. Similarly, the Ninth Circuit has held California may
 20 not regulate “sales that take place outside California” merely because the seller resides in
 21 California. *Sam Francis Found. v. Christies, Inc.*, 784 F.3d 1320, 1323 (9th Cir. 2015).

22 As in these cases, Illinois may not regulate a company’s conduct involving biometric data
 23 that occurs entirely outside Illinois. “One state cannot be permitted to dictate what other states
 24 must do within their own borders.” *Daniels Sharpsmart*, 889 F.3d at 615. Illinois cannot dictate
 25 whether Microsoft may lawfully download a dataset with biometric information within
 26 Washington or New York. Yet that is precisely the outcome Plaintiffs demand here. The Court
 27 should reject Plaintiffs’ invitation to apply BIPA in an unconstitutional manner and, instead, hold

1 BIPA's application to Microsoft on these facts would violate the dormant Commerce Clause.

2 **2. BIPA's Application Here Would Conflict with Washington and New**
 3 **York Biometric Privacy Law.**

4 In addition, applying BIPA here would conflict with the policy and legislative decisions
 5 of Washington and New York concerning biometric data. Washington enacted its own
 6 Biometric Privacy Law where it expressly exempted "data generated" from "a physical or digital
 7 photo" from its protections. RCW 19.375.010(1). Washington has also chosen to extend privacy
 8 protections only to the use and collection of biometric information for "commercial purposes."
 9 RCW 19.375.020(1). Because Skrainka and Samadi each downloaded the DiF Dataset for
 10 research purposes only, the "commercial purposes" limitation in Washington law would exclude
 11 Microsoft's download of the Dataset.⁷ Unlike Illinois, Washington requires notice and consent
 12 only to "enroll" biometric information in a database, which involves "captur[ing] a biometric
 13 identifier of an individual, convert[ing] it into a reference template that cannot be reconstructed
 14 into the original output image, and stor[ing] it in a database that matches the biometric identifier
 15 to a specific individual. RCW 19.375.020; RCW 19.375.101(5). Plaintiffs do not allege
 16 Microsoft engaged in any such "enrollment" activity. Rather, they hinge their liability theory on
 17 Microsoft downloading a dataset in which IBM included data generated from some of the
 18 photos—conduct the Washington law would, again, exclude. Microsoft fully complied with
 19 Washington law, the jurisdiction where Skrainka interacted with the IBM DiF Dataset. The
 20 Court should not allow Plaintiffs to import Illinois' policy decisions into Washington to find a
 21 violation where Washington law would hold there was none.

22 Similarly, New York has chosen not to regulate use of biometric information, leaving that
 23 information freely available for use by companies and researchers. New York City (effective
 24 July 9, 2021) passed a biometric privacy law, to apply only to a "commercial establishment"—

26 ⁷ "Commercial purpose" means "in furtherance of the sale or disclosure to a third party of a biometric identifier for
 27 the purpose of marketing of goods or services when such goods or services are unrelated to the initial transaction in
 which a person first gains possession of an individual's biometric identifier." RCW 19.375.010(4). In other words,
 Washington's biometric privacy statute applies only to the sale or disclosure of biometric information itself.

defined to mean “a place of entertainment, a retail store, or a food and drink establishment,” New York City Code § 22-1201—that “collects, retains, converts, stores or shares biometric identifier information of customers,” and allows the free transfer of biometric information, although it cannot be sold. New York City Code § 22-1202. Plaintiffs have no argument that IBM’s (or Microsoft’s) conduct would have violated New York City’s biometric privacy law, even if the law had been in effect when Samadi downloaded the DiF Dataset in 2019.

Applying BIPA to Microsoft’s wholly out-of-state conduct here would effectively allow Illinois to make policy and legislative decisions for Washington and New York, substituting its views for the different biometric privacy policy decisions of these other states. It is no answer to suggest that Microsoft could comply with the stricter law. In that event, Illinois would still be overruling other states’ chosen biometric policies, including (a) Washington’s decision to allow use of all biometric information for non-commercial purposes and to allow the use of biometric data derived from photos for any purposes, and (b) New York’s decision not to regulate at all. *Cf. Nat’l Collegiate Athletic Ass’n v. Miller*, 10 F.3d 633, 639-40 (9th Cir. 1993), *overruled on other grounds by Olean Wholesale Grocery Coop., Inc. v. Bumble Bee Foods LLC*, 31 F.4th 651 (9th Cir. 2022) (rejecting a “comply with the most stringent” argument); *see also Mazza v. Am. Honda Co., Inc.*, 666 F.3d 581, 592 (9th Cir. 2012) (recognizing that states may choose to leave some conduct unregulated in “balancing the competing interests” between promoting business and protecting consumers).

The Court denied Microsoft’s dormant Commerce Clause arguments at the motion to dismiss stage, explaining it “need[ed] more information about the technology behind how Microsoft obtained, stores, or uses the Diversity in Faces dataset[.]” Dkt. 43 at 11. The Court now has that information. Microsoft obtained the DiF Dataset when Skrainka, in Washington, and Samadi, in New York, each downloaded it from IBM servers in New York, solely to evaluate the possible use of photos linked in the Dataset for research purposes. Neither had any interest in IBM’s facial annotations. Skrainka Decl. ¶¶ 5-6; Skrainka Dep. 208-:3-15; Samadi Decl. ¶ 6-8; Samadi Dep. 177:15-178:1; Vaughan Decl. ¶ 6. Nothing is complex about the

technology—the download operated in the way that any download from an online link would. Merler Decl. ¶ 10. Microsoft did not use the Dataset. Samadi Decl. ¶¶ 7, 12; Skrainka Decl. ¶¶ 7, 12; Kasap Decl. ¶¶ 7-8; Vaughan Decl. ¶¶ 7, 10. Skrainka and Samadi examined some photos in the DiF Dataset briefly but found them useless and abandoned the Dataset. They did nothing with the DiF Dataset—they did not incorporate it into or use it to improve any Microsoft product. Nor did anyone else. Kasap Decl. ¶ 7; Bruncke Decl. ¶ 7; Bruncke Dep. 64:7-19; Vaughan Decl. ¶¶ 7, 10; Vaughan Dep. 56:5-16; Samadi Decl. ¶¶ 7, 12; Skrainka Decl. ¶¶ 7, 12; Skrainka Dep. 251:12-23.

None of Microsoft’s relevant conduct occurred in Illinois, and the Court should hold the dormant Commerce Clause bars BIPA from applying to Microsoft on these facts.

II. BIPA Section 15(b) Does Not Apply Because Microsoft Had No Way To Give Notice and Obtain Consent Before Downloading The DiF Dataset.

Setting aside the extraterritoriality and dormant Commerce Clause issues, BIPA’s notice-and-consent provision, 740 ILCS 14/15(b), does not apply when a company has no relationship with, does not know, and has no practical means of contacting the individuals whose anonymous biometric information appears in a dataset the company downloads but does not use. *See Zellmer*, 2022 WL 976981, at *3.

Plaintiffs’ only remaining BIPA claim arises under Section 15(b), which prohibits a private entity from collecting or obtaining biometrics without first giving notice to and obtaining consent from the “subject.” 740 ILCS 14/15(b). This requirement plainly regulates businesses that collect biometric information from employees, customers, or site visitors. But Section 15(b) cannot be read to impose onerous research and notice requirements on businesses or academic institutions seeking to acquire a legitimate dataset with publicly available photographs of unknown persons, along with annotations of some of the faces depicted. To the contrary, the Illinois Supreme Court has emphasized that “compliance” with BIPA “should not be difficult,” so that “whatever expenses a business might incur to meet the law’s requirements are likely to be insignificant.” *Rosenbach v. Six Flags Entertainment*, 129 N.E.3d 1197, 1207 (Ill. 2019).

1 The BIPA “compliance” Plaintiffs demand of Microsoft is not just “difficult” but
 2 practically impossible, to the point where application of Section 15(b) would be absurd.
 3 Microsoft obtained a dataset with links to publicly-available photos of people from around the
 4 world, without knowing whether *any* of those people were from Illinois. Samadi Decl. ¶¶ 8, 9;
 5 Samadi Dep. 177:15-178:1, 257:1-5; Skrainka Decl. ¶¶ 6, 10; Skrainka Dep. 358:17-23. To the
 6 extent the DiF Dataset included Illinois residents’ information, Microsoft could not identify them
 7 among the one million photos, discern which of them had annotations of their faces in the
 8 Dataset, provide them with notice, and solicit a release—much less do so *before* downloading the
 9 Dataset. Plaintiffs’ suggestions for class notice illustrate the point, proposing Rube Goldberg-
 10 like research and notice processes that no reasonable business or academic institution could
 11 practically undertake before downloading a dataset. *See* Dkt. 79 (Opp. to Class Cert.) at 10:1-
 12 12:24. The effect of applying Section 15(b) on these facts would be to deter persons (including
 13 academic researchers like Samadi) from interacting with *any* dataset of facial images of
 14 unidentified subjects, lest they be exposed unwittingly to BIPA’s penalties.

15 Nothing suggests the Illinois legislature intended that absurd result. The General
 16 Assembly focused on collection of biometrics through business interactions, such as “at grocery
 17 stores, gas stations, and school cafeterias,” 740 ILCS 14/5(b), and use of biometrics in “financial
 18 transactions and security screenings,” 740 ILCS 14/5(a). Section 15(b) cannot be read to require
 19 business and academia to research the residence of every anonymous person whose biometrics
 20 appear in a dataset, and then track them down to secure consent *before* downloading the dataset.

21 The court reached this same conclusion in *Zellmer*, 2022 WL 976981, at *3. Plaintiff
 22 accused Facebook of violating BIPA by scanning user-uploaded photos to identify non-Facebook
 23 users. *Id.* at *1. Plaintiff was not a Facebook user; he simply appeared in photos Facebook users
 24 uploaded to the site. *Id.* He sued on behalf of Illinois non-Facebook users, alleging Facebook
 25 needed to notify him and obtain consent before scanning his image. *Id.* The court granted
 26 summary judgment on plaintiff’s Section 15(b) claim because Facebook had no realistic way,
 27 and no obligation, to provide notice to unknown non-Facebook users. *Id.* at *4. The court held

that BIPA applies only where there is a “minimum level of known contact” between a person and the entity who collects biometric information. *Id.* at *4. Construing BIPA otherwise “would lead to obvious and insoluble problems.” *Id.* For example, Facebook would somehow need to identify every non-user in Illinois and find a way to communicate with them to provide notice and obtain consent. *Id.* The court found the Illinois legislature could not have intended such an absurd result. *Id.* at *5; *see also People v. Hanna*, 207 Ill. 2d 486, 498 (2003) (“It is a familiar rule, that a thing may be within the letter of the statute and yet not within the statute, because not within its spirit, nor within the intention of its makers.”).

The same principles apply even more forcefully here, where Microsoft (unlike Facebook) had nothing to do with creation of the dataset allegedly containing Plaintiffs’ information and no relationship with Plaintiffs; it simply downloaded a dataset. It would be “patently unreasonable to construe BIPA to mean that [Microsoft] was required to provide notice to, and obtain consent from, non-users who were for all practical purposes total strangers to [Microsoft], and with whom [Microsoft] had no relationship whatsoever.” *Zellmer*, 2022 WL 976981, at *3. In addition to putting Microsoft in the “impossible position” of identifying and communicating with potentially thousands of people with whom it had no relationship and no ability to locate, *id.* at *5, Plaintiffs’ theory would stretch BIPA beyond any reasonable bounds.⁸ The Court should grant summary judgment on the Section 15(b) claim on this additional basis.

III. The Court Should Grant Summary Judgment on the Unjust Enrichment Claim.

Plaintiffs allege Microsoft obtained a “monetary benefit” from them to their detriment, and that it did so by “profiting off of Plaintiffs’ ... biometric identifiers and information.” Compl. ¶ 108. But the undisputed evidence establishes that Microsoft did not use the DiF Dataset at all. It therefore did not and could not possibly have obtained any “monetary benefit”

⁸ The Court refused at the pleading stage to “require some relationship to exist” between Microsoft and Plaintiffs as predicate to Section 15(b) liability, based in part on two Northern District of Illinois cases. Dkt. 43 at 19. But the defendants in those cases had actually extracted and created the purported biometrics, even though plaintiffs had no relationship with defendants. By contrast, Microsoft did *nothing* to extract, create, or even view the data that Plaintiffs complain about. In light of the fully developed record and the persuasive reasoning in *Zellmer*, the Court should construe BIPA to not require notice and consent in these circumstances.

1 or “profit” from Plaintiffs’ biometric identifiers or information.

2 In denying Microsoft’s motion to dismiss the unjust enrichment claim, the Court held that
3 Illinois law governed this claim because Plaintiffs allegedly uploaded their photos in Illinois.
4 Dkt. 47 at 16 (“uploaded Illinois-created content in Illinois”; “the benefiting act (the sharing of
5 facial images) was done [in Illinois]”). Under Illinois law, “a plaintiff must allege that the
6 defendant has unjustly retained a benefit to the plaintiff’s detriment, and that defendant’s
7 retention of the benefit violates the fundamental principles of justice, equity, and good
8 conscience.” *Cleary v. Philip Morris Inc.*, 656 F.3d 511, 516 (7th Cir. 2011) (citation omitted).

9 Attempting to satisfy the elements of unjust enrichment under Illinois law, Plaintiffs
10 alleged that Microsoft benefited because it used the DiF Dataset to “improve its facial
11 recognition products.” Compl. ¶ 58. But the evidence demonstrates that this allegation has no
12 factual basis. Microsoft did not use or benefit from the Dataset, much less “profit” from it.
13 Skrainka and Samadi each reviewed some linked photos briefly, but neither they nor anyone else
14 at Microsoft used the DiF Dataset for any purpose—much less used the annotations that
15 Plaintiffs claim are biometrics. Samadi Decl. ¶¶ 7, 12; Samadi Dep. 177:15-178:1; Skrainka
16 Decl. ¶¶ 7, 12; Skrainka Dep. 231:13-232:14; Kasap Decl. ¶¶ 7-8; Vaughan Decl. ¶¶ 7,10;
17 Vaughan Dep. 56:5-16. Because Microsoft obtained no “benefit” from the DiF Dataset, the
18 Court should grant summary judgment on Plaintiffs’ unjust enrichment claim.⁹

19 CONCLUSION

20 For the foregoing reasons, Microsoft respectfully requests that the Court grant summary
21 judgment on Plaintiffs’ two remaining claims.

22
23
24
25 ⁹ In its Motion to Dismiss, Microsoft argued that Washington law should apply under a choice of law analysis.
26 Under Washington law, Plaintiffs must show “(1) [Microsoft] received a benefit, (2) at [Plaintiffs’] expense, and (3)
27 the circumstances make it unjust for [Microsoft] to retain the benefit without payment.” *Cousineau v. Microsoft Corp.*, 992 F. Supp. 2d 1116, 1129 (W.D. Wash. 2012). For the same reasons Plaintiffs’ claim fails under Illinois law, it fails under Washington law. Similarly, to the extent New York law applies to Samadi’s download in New York, Plaintiffs’ claim also fails under New York law. Plaintiffs do not suggest Microsoft, “has received money to which [it] is not entitled.” *Corsello v. Verizon New York, Inc.*, 967 N.E.2d 1177, 1185 (N.Y. 2012).

1 DATED this 19th day of May, 2022.

2 DAVIS WRIGHT TREMAINE LLP
3 Attorneys for Defendant Microsoft Corporation

4 By /s/ Stephen M. Rummage
5 Stephen M. Rummage, WSBA #11168
6 Xiang Li, WSBA #52306
7 920 Fifth Avenue, Suite 3300
8 Seattle, WA 98104-1610
9 Telephone: (206) 757-8136
10 Fax: (206) 757-7136
11 E-mail: steverummage@dwt.com
12 xiangli@dwt.com

13 MORGAN LEWIS & BOCKIUS
14 Attorneys for Defendant Microsoft Corporation

15 By /s/ Elizabeth B. Herrington
16 Elizabeth B. Herrington (*pro hac vice*)
17 Phillip J. Wiese (*pro hac vice*)
18 110 North Wacker Drive, Suite 2800
19 Chicago, IL 60606-1511
20 Telephone: (312) 324-1000
21 E-mail: beth.herrington@morganlewis.com
22 phillip.wiese@morganlewis.com
23
24
25
26
27